

REMARKS

Upon entry of this amendment, claims 1-31, 34 and 35 are all the claims pending in the application. Claims 32 and 33 have been canceled by this amendment.

Applicants note that a number of editorial amendments have been made to the specification and abstract for grammatical and general readability purposes. Due to the number of changes made, a substitute specification and abstract are submitted herewith. No new matter has been added. Also enclosed is a marked-up copy of the original specification and abstract showing the changes incorporated into the substitute specification and abstract.

I. Information Disclosure Statement

In item 2 on page 2 of the Office Action, the Examiner has indicated that the two non-patent literature publications filed with the IDS of March 30, 2004 have not been considered because copies were not supplied.

Regarding these references, Applicants are enclosing herewith the stamped postcard receipt from the PTO which shows that all of the references submitted with the IDS of March 30, 2004 were received by the PTO. For the Examiner's convenience, however, Applicants are resubmitting copies of the above-noted non-patent literature references herewith.

In view of the foregoing, Applicants kindly request that the Examiner consider the references submitted with the IDS of March 30, 2004, and return the initialed and signed PTO-1449 form with the next Office paper.

II. Objections to the Specification

The Examiner has objected to the specification because NTRU was not identified in the specification as a registered trademark. By this amendment, Applicants have modified the specification so as to properly identify “NTRU” as a registered trademark. Accordingly, Applicants kindly request the objection be reconsidered and withdrawn.

In addition, the Examiner has objected to the specification because it contains embedded hyperlinks. Applicants have modified the specification so as to remove all instances of embedded hyperlinks, and therefore, kindly request that the above-noted objection be withdrawn.

III. Claim Rejections under 35 U.S.C. § 101

The Examiner has rejected claims 32-35 under 35 U.S.C. §101 as allegedly being directed to non-statutory subject matter.

Regarding claims 32 and 33, Applicants note that these claims have been canceled.

Regarding claims 34 and 35, Applicants note that in order to further clarify that these claims are drawn to statutory subject matter, claim 34 has been amended by adding the feature of “an outputting step of outputting the encrypted text”, and claim 35 has been amended by adding the feature of “an outputting step of outputting the decrypted text”.

Further, with respect to the Examiner’s indication that claims 34 and 35 are directed to a program listing having no functional interrelationship, Applicants note that the MPEP describes non-functional descriptive material as being material such as music, literary works,

compilations of data, or mere arrangements of data (see MPEP 2106.01, first paragraph).

Such material cannot be employed as a computer component, and does not impart any functionality. In contrast, functional descriptive material includes computer programs which impart functionality when employed as a computer component (see MPEP 2106.01, first paragraph).

Moreover, Applicants note that the MPEP indicates that “a claimed computer readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program’s functionality to be realized, and is thus statutory” (see MPEP 2106.01(I), second paragraph)(emphasis added).

In this regard, Applicants note that claim 34 is drawn to a computer-readable storage medium on which an encryption program for generating an encrypted text is recorded, the encryption program causing a computer to perform the steps recited in the body of the claim. By causing the computer to perform such steps, the encryption program of claim 34 is clearly to be employed as a computer component, and as such, imparts the function of generating an encrypted text, and thus permits the computer program’s functionality to be realized.

Each of the steps recited in the body of claim 34 constitute the functions imparted by the computer program which is employed as a computer component by causing the computer to perform such steps. Thus, the encryption program of claim 34 is employed as a computer component and imparts the functions of causing the computer to generate the encrypted text from the plaintext, using an encryption key and a parameter, according to an encryption

algorithm which changes the probability of decryption error in decrypting the encrypted text depending on a value of the parameter adapted to a decryption apparatus; updating the parameter; and outputting the encrypted text.

As is evident from the above-noted features recited in claim 34, Applicants respectfully submit that such features cannot merely be considered as “non-functional” descriptive material, but instead, clearly define functional interrelationships between the computer program and the rest of the computer which permit the computer program’s functionality to be realized. Accordingly, Applicants submit that claim 34 is statutory under 35 U.S.C. 101, and therefore, kindly request that the Examiner reconsider and withdraw the rejection.

Regarding claim 35, Applicants note that this claim is drawn to a computer-readable storage medium on which a decryption program for decrypting an encrypted text is recorded, wherein the decryption program causes a computer to execute the steps of generating a decrypted text using a decryption key, from the encrypted text generated according to an encryption algorithm which changes a probability of decryption error in decrypting the encrypted text depending on a value of a parameter; judging whether or not the decrypted text is obtained correctly; requesting an encryption apparatus to update the decryption key, according to a result of the judgment in the judgment step; requesting the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of the decryption error to a value less than or equal to a predetermined value, according to the result of the judgment in the judgment step; and outputting the decrypted text.

For at least similar reasons as discussed above with respect to claim 34, Applicants respectfully submit that the above-noted features recited in claim 35 cannot merely be considered as “non-functional” descriptive material, but instead, define functional interrelationships between the computer program and the rest of the computer which permit the computer program’s functionality to be realized. Accordingly, Applicants submit that claim 35 is statutory under 35 U.S.C. 101, and therefore, kindly request that the Examiner reconsider and withdraw the rejection.

IV. Claim Rejections under 35 U.S.C. § 112, second paragraph

The Examiner has rejected claims 2, 4, 7, 11, 19, 20, 27 and 30 under 35 U.S.C. § 112, second paragraph as being indefinite due to the use of the phrase “as time goes by”. By this Amendment, Applicants note that the above-noted phrase has been removed from the claims, and therefore, kindly request that the rejection be withdrawn.

V. Claim Rejections under 35 U.S.C. § 102

A. Claims 1, 2, 7, 13, 26, 27, 32 and 34 were rejected under 35 U.S.C. § 102(b) as being anticipated by DeBellis (U.S. 6,104,810). Applicants respectfully traverse this rejection on the following basis.

Claim 1 recites the feature of a storage unit operable to store an encryption key and a parameter, the parameter being used to change a probability of decryption error in decrypting encrypted text. Applicants respectfully submit that DeBellis does not disclose or suggest at

least this feature of claim 1.

Regarding the above-noted feature recited in claim 1, the Examiner has taken the position in the Office Action that DeBellis discloses such a feature at col. 5, lines 40-51 (see Office Action at page 5). Applicants respectfully disagree.

In particular, Applicants note that this section of DeBellis indicates that in order to provide integrity and secrecy, periodic backup of hardware information to non-volatile storage is coupled with additional appropriate feedback, update and restoration algorithms (see col. 5, lines 40-44). Regarding the backup of the hardware information, DeBellis discloses that a current-value of a time-dependent value is used as a backup time-dependent value, and that a hash of a current secret value is used as a backup secret value (see col. 5, lines 45-51). As explained in DeBellis, this minimizes the possibility of restoration resulting in repetition of pseudorandom numbers (see col. 5, lines 51-52).

Based on the foregoing description of DeBellis, Applicants note that while DeBellis discloses a backup routine for storing hardware information that minimizes the possibility of restoration resulting in the repetition of a pseudorandom number, that DeBellis does not disclose or in any way suggest the feature of a storage unit that is operable to store a parameter which is used to change a probability of decryption error in decrypting encrypted text.

In view of the foregoing, Applicants respectfully submit that DeBellis does not disclose, suggest or otherwise render obvious at least the above-noted feature recited in claim 1. Accordingly, Applicants submit that claim 1 is patentable over DeBellis, an indication of which is kindly requested.

In addition, Applicants note that claim 1 also recites the feature of an encryption unit that is operable to generate the encrypted text from the plaintext, using the encryption key and the parameter stored in the storage unit, according to an encryption algorithm which changes the probability of the decryption error in decrypting the encrypted text depending on a value of the parameter. Applicants respectfully submit that DeBellis also does not disclose or suggest this feature of claim 1.

Regarding the above-noted feature, Applicants note that the Examiner has taken the position in the Office Action that DeBellis discloses such a feature at col. 12, lines 15-26 (see Office Action at page 5). Applicants respectfully disagree.

In particular, Applicants note that this section of DeBellis cited by the Examiner merely discloses the use of an encryption function which utilizes an encryption key to encrypt plaintext data using Data Encryption Algorithm (DEA), also referred to as Data Encryption Standard (DES), in order to generate a 64-bit ciphertext value (see col. 12, lines 16-23).

Thus, while this section of DeBellis discloses the ability to perform encryption using a well known encryption algorithm (DES) for generating ciphertext, Applicants respectfully submit that such disclosure does not in any way suggest that encryption takes place according to an encryption algorithm which changes the probability of the decryption error in decrypting the encrypted text depending on a value of the parameter.

In view of the foregoing, Applicants respectfully submit that DeBellis does not disclose, suggest or otherwise render obvious all of the features recited in claim 1. Accordingly, Applicants submit that claim 1 is patentable over DeBellis, an indication of

which is kindly requested.

Claims 2, 7 and 13 depend from claim 1 and are therefore considered patentable at least by virtue of their dependency.

Regarding claims 26 and 34, Applicants note that each of these claims recites the feature of an encrypted text generating step of generating the encrypted text from the plaintext, using an encryption key and a parameter, according to an encryption algorithm which changes a probability of decryption error in decrypting the encrypted text depending on a value of the parameter adapted to a decryption apparatus.

For at least similar reasons as discussed above with respect to claim 1, Applicants submit that DeBellis does not disclose, suggest or otherwise render obvious such a feature. Accordingly, Applicants submit that claims 26 and 34 are patentable over DeBellis, an indication of which is kindly requested. Claim 27 depends from claim 26 and is therefore considered patentable at least by virtue of its dependency.

B. Claims 14, 17, 31, 33 and 35 were rejected under 35 U.S.C. § 102(b) as being anticipated by Geiringer (WO 01/93013). Applicants respectfully traverse this rejection on the following basis.

Claim 14 recites the features of a decryption key updating request unit operable to request an encryption apparatus to update the decryption key, according to a result of a judgment made by the judgment unit. Applicants respectfully submit that Geiringer does not disclose or suggest at least this feature of claim 14.

Regarding the above-noted feature recited in claim 14, the Examiner has taken the position in the Office Action that Geiringer discloses such a feature at page 28, lines 12-20 (see Office Action at page 7). Applicants respectfully disagree.

In particular, Applicants note that this section of Geiringer indicates that if a transmitted check block does not match a previously created hash, then the decoded polynomial is not the original i^{th} message polynomial, and in such a case, error correction can be performed in order to recover the original message polynomial, wherein the error correction system reports back its success (see page 28, lines 12-20).

Based on the foregoing description, Applicants note that, in Geiringer, while it is possible to perform error correction to recover an original message polynomial, that the mere recovery of an original message polynomial does not correspond to an update of a decryption key. In other words, in Geiringer, even if an original message polynomial is recovered, this would not result in the update of a decryption key.

In view of the foregoing, Applicants respectfully submit that Geiringer does not disclose, suggest or otherwise render obvious at least the above-noted feature recited in claim 14. Accordingly, Applicants submit that claim 14 is patentable over Geiringer, an indication of which is kindly requested.

Further, Applicants note that claim 14 also recites the feature of a parameter initialization request unit operable to request the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of the decryption error in decrypting the encrypted text to a value less than or equal to a predetermined value.

Applicants respectfully submit that Geiringer does not disclose or suggest such a feature.

Regarding the above-noted feature recited in claim 14, the Examiner has taken the position in the Office Action that Geiringer discloses such a feature at page 28, lines 18-20 (see Office Action at page 7). Applicants respectfully disagree.

In particular, Applicants note that this section of Geiringer merely indicates that if error correction is successful in recovering an original message polynomial, then a different decoded polynomial, b_i , is accepted as the next message polynomial and the cipher continues as normal (see page 28, lines 18-20). In other words, when error correction successfully recovers an original message polynomial, the cipher continues as normal by accepting the next message polynomial, where the next message polynomial will naturally have a different value than the previous message polynomial.

Thus, while the above-noted section of Geiringer relates to the cipher continuing in a normal manner after error correction is performed, Applicants respectfully submit that this disclosure does not in any way relate to an encryption apparatus being requested to change the value of a parameter to an initial value which decreases the probability of the decryption error in decrypting the encrypted text.

In view of the foregoing, Applicants respectfully submit that Geiringer does not disclose, suggest or otherwise render obvious at least the above-noted feature recited in claim 14. Accordingly, Applicants submit that claim 1 is patentable over Geiringer, an indication of which is kindly requested. Claim 17 depends from claim 14 and is therefore considered patentable at least by virtue of its dependency.

Regarding claims 31 and 35, Applicants note that each of these claims recites the features of an updating request step of requesting an encryption apparatus to update the decryption key, according to a result of the judgment in the judgment step; and an initialization request step of requesting the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of decryption error to a value less than or equal to a predetermined value, according to the result of the judgment in the judgment step.

For at least similar reasons as discussed above with respect to claim 14, Applicants submit that Geiringer does not disclose, suggest or otherwise render obvious such features. Accordingly, Applicants submit that claims 31 and 35 are patentable over Geiringer, an indication of which is kindly requested.

VI. Claim Rejections under 35 U.S.C. § 103(a)

A. Claims 3-5, 10, 11, 18-20, 25, 29 and 30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over DeBellis et al. (U.S. 6,104,810) in view of Geiringer (WO 01/93013).

Claim 18 recites the features of an encryption apparatus that includes a storage unit operable to store an encryption key and a parameter, the parameter being used to change a probability of decryption error in decrypting the encrypted text; an encryption unit operable to generate the encrypted text from the plaintext, using the encryption key and the parameter stored in the storage unit, according to an encryption algorithm which changes the probability of the decryption error in decrypting the encrypted text depending on a value of the parameter;

and a decryption apparatus that includes a decryption key updating request unit operable to request the encryption apparatus to update the decryption key; and a parameter initialization request unit operable to request the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of the decryption error to a value less than or equal to a predetermined value.

For at least similar reasons as discussed above with respect to claims 1 and 14, Applicants submit that DeBellis and Geiringer, either alone or in combination, do not disclose, suggest or otherwise render obvious such features. Accordingly, Applicants submit that claim 18 is patentable over DeBellis and Geiringer, an indication of which is kindly requested. Claims 19, 20 and 25 depend from claim 18 and are therefore considered patentable at least by virtue of their dependency.

Regarding claims 3-5, 10, 11, 29 and 30, Applicants note that claims 3-5, 10 and 11 depend from claim 1, and claims 29 and 30 depend from claim 26. Applicants respectfully submit that Geiringer does not cure the deficiencies of DeBellis, as noted above, with respect to claims 1 and 26. Accordingly, Applicants submit that claims 3-5, 10, 11, 29 and 30 are patentable at least by virtue of their dependency.

B. Claims 8, 9, 22 and 28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over DeBellis et al. (U.S. 6,104,810) in view of Nishio et al. (U.S. 5,848,154).

Claims 8 and 9 depend from claim 1; claim 22 depends from claim 18; and claim 28 depends from claim 26. Applicants respectfully submit that Nishio does not cure the

deficiencies of DeBellis, as noted above, with respect to claims 1, 18 and 26. Accordingly, Applicants submit that claims 8, 9, 22 and 28 are patentable at least by virtue of their dependency.

In addition, regarding claims 8 and 22, Applicants note that these claims recite that the updating unit updates the parameter stored in the storage unit according to the number of times the encryption unit performs encryption. In the Office Action, the Examiner has taken the position that Nishio discloses such a feature at col. 3, lines 22-35. Applicants respectfully disagree.

In particular, Applicants note that while Nishio discloses at col. 3, lines 22-35 that it is determined whether a software using quantity is reached, that Nishio does not disclose or in any way suggest that an updating unit updates a parameter according to the number of times encryption is performed.

In view of the foregoing, Applicants respectfully submit that the cited prior art does not disclose, suggest or otherwise render obvious all of the features recited in claims 8 and 22. Accordingly, Applicants submit that claims 8 and 22 are patentable over the cited prior art, an indication of which is kindly requested.

C. Claims 15 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Geiringer (WO 01/93013) in view of Nishio et al. (U.S. 5,848,154).

Claims 15 and 16 depend from claim 14. Applicants respectfully submit that Nishio does not cure the deficiencies of Geiringer, as noted above, with respect to claim 14.

Accordingly, Applicants submit that claims 15 and 16 are patentable at least by virtue of their dependency.

D. Claims 6, 21 and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over DeBellis et al. (U.S. 6,104,810) in view of Geiringer (WO 01/93013) and further in view of Nishio et al. (U.S. 5,848,154).

Claim 6 depends from claim 1, and claims 21 and 24 depend from claim 18. Applicants respectfully submit that Nishio does not cure the deficiencies of DeBellis as Geiringer, as noted above, with respect to claims 1 and 18. Accordingly, Applicants submit that claims 6, 21 and 24 are patentable at least by virtue of their dependency.

E. Claim 12 was rejected under 35 U.S.C. § 103(a) as being unpatentable over DeBellis et al. (U.S. 6,104,810) in view of Geiringer (WO 01/93013), and further in view of Whyte ("Analysis of NTRUEncrypt Paddings, STRONG security that fits everywhere," NTRU, August 2002).

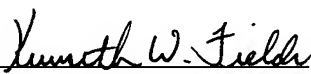
Claim 12 depends from claim 1. Applicants respectfully submit that Whyte does not cure the deficiencies of DeBellis and Geiringer, as noted above, with respect to claim 1. Accordingly, Applicants submit that claim 12 is patentable at least by virtue of their dependency.

VII. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Masato YAMAMICHI et al.

By: 
Kenneth W. Fields
Registration No. 52,430
Attorney for Applicants

KWF/jjv
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
May 29, 2007